

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-103425

(43)Date of publication of application : 15.04.1994

(51)Int.Cl.

G06K 17/00  
G06F 9/06  
G06K 19/073

(21)Application number : 04-249293

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 18.09.1992

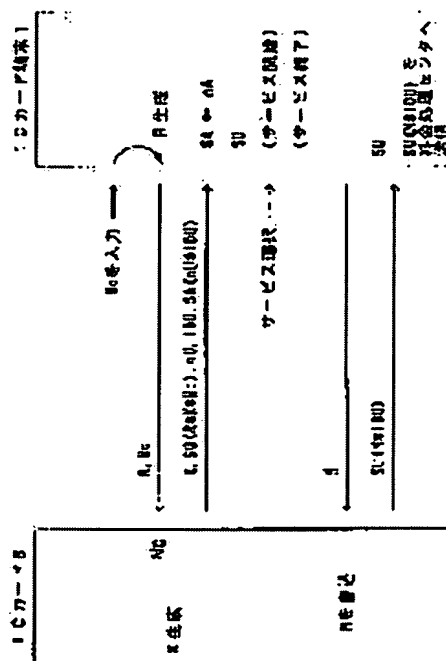
(72)Inventor : MUTA TOSHIYASU  
ISHIGURO GINYA  
SAKIDA KAZUTAKA  
MIYAGUCHI SHOJI  
OKAMOTO TATSUAKI  
FUJIOKA ATSUSHI

## (54) IC CREDIT CARD SYSTEM

## (57)Abstract:

PURPOSE: To make it unnecessary to access a center during the supply of service, and in addition, to improve safety.

CONSTITUTION: When a user inserts an IC card 6 into a terminal 1, and inputs a pass word Nc, a random number R is generated at the terminal 1, and the IC card 6 receives this, and when it coincides with the stored password, it generates the random number X, and produces a digital signature SU, and sends a stored digital signature SA of a card issuer corresponding to card device information IDU and the opening key nU of the card and these to the terminal 1. The terminal 1 verifies reception by using the stored opening key nA, and if it is correct, it makes user service start, and the terminal 1 transmits service information M such as a service charge and a date, etc., to the IC card 6. The IC card 6 stores this M in a memory, and simultaneously, it produces the digital signature SU, and sends it to the terminal 1. The terminal 1 verifies this, and if it is correct, it stores it in the memory, and it transmits the stored M service information etc., to the center at every definite period or every time data becomes some definite quantity.



## LEGAL STATUS

[Date of request for examination]

14.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-103425

(43)公開日 平成6年(1994)4月15日

(51)Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00		T 7459-5L		
G 0 6 F 9/06	4 5 0 B	9367-5B		
G 0 6 K 19/073		8623-5L	G 0 6 K 19/ 00	P

審査請求 未請求 請求項の数2(全 9 頁)

(21)出願番号 特願平4-249293

(22)出願日 平成4年(1992)9月18日

(71)出願人 000004226

日本電信電話株式会社  
東京都千代田区内幸町一丁目1番6号(72)発明者 牟田 敏保  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内(72)発明者 石黒 銀矢  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内(72)発明者 崎田 一貴  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内

(74)代理人 弁理士 草野 卓

最終頁に続く

(54)【発明の名称】 ICクレジットカードシステム

(57)【要約】 (修正有)

【目的】 サービス提供中にセンタにアクセスする必要がなく、かつ安全性が極めて高い。

【構成】 利用者がICカードを端末に挿入してパスワードNcを入力すると、端末に乱数Rを生成して、ICカードへ送信する。ICカードは受信して記憶してあるパスワードと一致すると、乱数Xを生成し、デジタル署名SUを作成し、記憶してある、カード装置情報IDUとカードの公開鍵nUに対するカード発行者のデジタル署名SAと、これらとを端末へ送信する。端末は記憶してある公開鍵nAを用いて受信を検証し、正しければ利用者サービスを開始させ、端末はサービス料金、日時などのサービス情報MをICカードへ送信する。ICカードはそのMをメモリに記憶すると共に、デジタル署名SUを作り、これを端末へ送信する。端末はこれを検証し、正しければメモリに記憶し、一定期間ごと、あるいは一定データ量になると、記憶してあるMサービス情報などをセンタへ送信する。

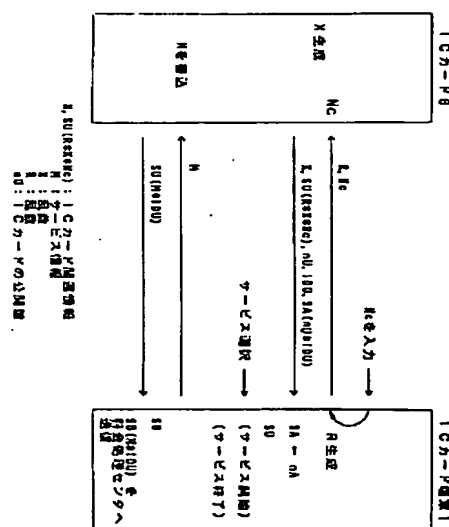


図2

## 【特許請求の範囲】

【請求項1】 乱数Xを発生する手段、ICカード端末から受信した乱数R及び前記Xを含む情報に対するICカードのデジタル署名SUを作成する手段、ICカードの公開鍵nU、ICカード特定情報IDUを含む情報に対するICカード発行者のデジタル署名SA、前記X、前記SU、前記nU、前記IDUをICカード端末へ送信する手段、ICカード端末から受信したサービス料金、サービス条件等のサービス情報Mと前記IDUを含む情報に対するICカードのデジタル署名SUを作成する手段、そのSUをICカード端末へ送信する手段を持つICカードと、

前記SU及びSAを受信し検証する手段、サービス終了後前記Mを作成し、ICカードへ送信する手段、及び前記SUを受信する手段を持つICカード端末とより成るICクレジットカードシステム。

【請求項2】 利用者が入力したパスワードをICカードへ送信する手段を前記ICカード端末に含み、ICカード端末から受信したパスワードを予めメモリに記録してあるパスワードと比較、検証する手段を前記ICカードに含むことを特徴とする請求項1記載のICクレジットカードシステム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 この発明は、予め識別番号などをセンタに登録してあるICカードをICカード端末へ利用者が挿入することによりサービスが提供されるICクレジットカードシステムに関し、特に極めてセキュリティ（安全性）が高く、サービス提供中にはセンタにアクセスする必要のないICクレジットカードシステムを得ようとするものである。

## 【0002】

【従来の技術】 従来、この種のシステムは、ICカードとICカード端末が同じ暗号方式で、同じ秘密鍵を持ち、互いに正しいICカード、ICカード端末であることを認証し、入力されたパスワードをICカード中のパスワードと照合し、ICカードからのICカード識別番号をICカード端末からICカードに関する識別番号などのデータベースを持つセンタへ送信し、センタで検証後、検証結果をICカード端末へ送信し、ICカード端末で結果が良好の場合はサービスを開始する方法がとられていた。あるいは、ICカードとセンタが直接、同じ秘密鍵による互いの認証を行う方法があった。

## 【0003】

【発明が解決しようとする課題】 従来のいずれの方法も、サービス提供前あるいは提供中に、センタとICカード端末が通信する必要があり、オンラインで検証するためセンタ設備が大規模になったり、通信料がサービスの他に加わったりする欠点があった。また、センタやICカードにサービスの履歴を残すことができるが、その

内容が不正に書込まれたものでないことを証明するのは困難であった。

【0004】 一方、文書に対し捺印するように、デジタル情報を発信した人が確かにその情報を発信し、認めたものであることを証明できるデジタル署名技術が例えば、NTT、R&D Vol. 40, No. 5, 1991, pp 687~686、「高速デジタル署名方式ESIGN」に示されるように確立されている。デジタル署名によれば、文書Mと秘密キーKを用い、署名生成関数により作成したデジタル署名Sを作成し、相手にこの署名Sと文書Mを送信し、相手は送信された文書M、署名Sと、公開キーUを用い、署名検証関数により確かに秘密キーKを持つ人による文書であるか否かを検証でき、秘密キーKを持つ人はその事実を否定できない。また、文書の一部変更しても、検証結果は不正と判定される。これらデジタル署名機能はESIGNと呼ばれるアルゴリズムを用いれば、ICカードに実装可能なプログラム規模で実用的処理時間に収まることが、前記文献に示されている。

【0005】 この発明の目的は前記デジタル署名を利用して、サービス提供中にセンタにアクセスする必要がなく、かつ極めて安全性が高いICクレジットカードシステムを提供することにある。秘密鍵Kを用いた文書Mと文書Nに対するデジタル署名をS(M\*N)と以下表記する。

## 【0006】

【課題を解決するための手段】 請求項1の発明によれば、乱数Xを発生する手段、ICカード端末から受信した乱数R及び前記Xを含む情報に対するICカードのデジタル署名SUを作成する手段、ICカードの公開鍵nU、ICカード特定情報IDUを含む情報に対するICカード発行者のデジタル署名SA、前記SU、前記X、前記nU、前記IDUをICカード端末へ送信する手段、ICカード端末から受信したサービス料金、サービス条件等のサービス情報Mを前記IDUを含む情報に対するICカードのデジタル署名SUを作成する手段、そのSUをICカード端末へ送信する手段を持つICカードと、前記SU及びSAを受信し検証する手段、サービス終了後前記Mを作成し、ICカードへ送信する手段、及び前記SUを受信する手段を持つICカード端末とよりICクレジットカードシステムが構成される。

## 【0007】

【作用】 このように構成されているから、発行者のデジタル署名付きのICカードを特定する情報がICカード端末で、検証できるので、ICカードに関するデータベースを持つセンタへサービス利用前にアクセスする必要がなく、不正なICカードによるサービス利用が排除できると共に、支払うべきサービス料金や、トラブルとなった時や利用者が参考とするための使用履歴などのサービス情報にそのICカードのデジタル署名を施して、I

Cカード端末へ送信し、ICカード端末は前記デジタル署名付きサービス情報を別途料金センタへ送信することにより、ICカードのデジタル署名付きのサービス情報がセンタに記録されるためにトラブル発生時には証拠として使用できる。

#### 【0008】

【実施例】次に図を参照してこの発明の実施例を説明する。図1にこの発明のシステム構成例を示す。ICカード6はあらかじめ図示していない発行機によって発行され、ICカード特定情報(IDU)及びその特定情報に対するICカード発行者のデジタル署名(SA(nU\*IDU))がEEPROMなどのメモリに記録されている。ここで、nUはICカード6によるデジタル署名SUを検証するための公開鍵である。またICカード6にはあらかじめパスワードNcが記録されている。ICカード6を特定する情報は料金処理センタ4に登録され、サービスを受けようとする時に、利用者がICカード6をICカード端末1あるいは2に挿入して、サービスを受ける。そのサービスを受けた後に、そのサービスについて料金処理センタ4でICカード別に料金処理が行われる。図1は通信網3を介して相手電話機5への通信サービスを受ける場合を示している。

【0009】図2は、この発明におけるICカード6とICカード端末1との間の情報の処理手順を示し、図3に、ICカード端末1の内部構成例を示し、図4に、ICカード6の内部構成例をそれぞれ示す。ICカード端末1は挿入されたICカード6に対する情報の読み出し、書き込みを行うICカードリードライト部11と、キーボードのような操作入力部12と、表示部13と、各部を制御する制御部14と、通信網3との通信を行う通信処理部15とよりなる。ICカード6においてはその処理手順、方法等のプログラムがROM61に記憶され、CPU63がワークエリアとしてRAM62を利用してすべての制御を行い、ICカード特定情報IDU、ICカード発行者のデジタル署名SAなどがEEPROM64に記憶され、通信部65は接点66を介してICカード端末1のICカードリードライト部11との通信を行う。

【0010】以下、この発明によるICクレジットカードシステムの動作を図を用いて説明する。ICカード6をICカード端末1のICカードリードライト部11へ挿入すると、ICカード端末1は表示部13にパスワードNcを入力するように利用者へガイダンス(表示)する。

【0011】利用者が操作入力部12よりパスワードNcを入力すると、そのパスワードNcとICカード端末1で生成した乱数RとをICカード6へ送信する。ICカード6ではそのNcとRを受信後、その受信したパスワードNcとあらかじめメモリに記憶してあるパスワードとを比較し、一致した場合は乱数Xを生成し、あらか

じめ発行時にICカード6のEEPROM64に記憶されているICカードのデジタル署名作成用秘密鍵を用いて、R、XとNcに対するデジタル署名SU(R\*X\*Nc)を作成し、ICカード関連情報即ち、乱数Xとデジタル署名SU(R\*X\*Nc)と、EEPROM64に記憶しているICカードのデジタル署名検証用公開鍵nU、ICカード特定情報IDUおよび、nUとIDUに対するICカード発行者のデジタル署名SA(nU\*IDU)を共にICカード端末1へ送信する。

【0012】ICカード端末1ではICカード端末設置時などあらかじめ制御部14に設定されてあるICカード発行者のデジタル署名用公開鍵nAを用いてデジタル署名SAを検証後、正しければ受信したnUを用いてデジタル署名SUを検証し、正しければ、サービス選択を行うように表示部13へガイダンスする。クレジット通話の場合は、利用者が相手電話機5のダイヤルを操作入力部12から入力し、通信網3を介して相手電話機5と通話が開始される。その通話が終了すると、サービス料金、日時、端末識別番号、サービスアクセス先等の問題が発生した時の参考となる情報や、利用者が後程確認したい情報であるサービス情報MをICカード6へ送信する。ICカード6ではサービス情報MをEEPROM64へ記憶し、さらにサービス情報MとICカード特定情報IDUに対してICカードのデジタル署名SUを施し、そのデジタル署名SU(M\*IDU)をICカード端末1へ送信する。ICカード端末1ではnUを用いてこのデジタル署名SU(M\*IDU)を検証し、正しければ一時、制御部14内のメモリに記憶し、例えば1週間毎に、あるいは一定量のデータが蓄積された時、または料金センタ4からボーリングがあった時に料金センタ4に通信網3を介して前記M、IDU、nU、SU(M\*IDU)を送信する。通信網3を介さずに携帯端末等をICカード端末1に接続して前記SU(M\*IDU)などを受信し、料金センタ4へ収集しても良い。料金センタ4ではデジタル署名SU(M\*IDU)をさらに検証して、ICカード特定情報IDU毎にサービス情報Mを記録して、利用者への料金請求や、問い合わせに使用する。

【0013】ICカード6及びICカード端末1の各情報の送信において、両方で特定の鍵を持ち、その鍵により情報を暗号化して送信し、受信側で鍵により復号化する方法をとれば回線の盗聴などに対するセキュリティ(安全性)を高めることができる。また、ICカードに有効期限情報を入れておき、ICカード端末内の時計により、ICカードの有効期限を検証するように構成すると紛失したICカードの不正使用に対して使用制限をもうけることができる。

【0014】さらに、ICカードに初期情報を記録するカード発行機の識別番号と、その識別番号に対するICカード発行者のデジタル署名、その署名の検証用公開鍵

5

をICカード発行時に記録しておくことにより、ICカードからICカード端末へこれらの情報を送信し、ICカード端末で検証することにより、正しいカード発行機で発行されたカードであることを確認することができる。

【0015】以上の説明では落としたICカードを使用できなくするため利用者がパスワードをICカード端末に入力させたが、サービスによって、あるいは利用者の希望により、パスワードなしでサービスすることも考えられ、この場合は、Ncがない形で図2に示した通信が行われる。さらに、以上の説明において、例えばnU、IDU、SA(nU\*IDU)で、nU\*IDUだけではデータ量が少なく、不正される可能性がある場合など実際のシステムでは、特に必要でないデータCを挿入して、nU、IDU、C、SA(nU\*IDU\*C)としてもよい。

【0016】

6

【発明の効果】以上述べたようにこの発明によれば、ICカードに発行者のデジタル署名が付いているので不正に製造されたICカードはICカード端末で拒否可能とすることができる。また、料金センタにICカードのデジタル署名付きサービス料金等の情報を記録することが可能であるから、そのようにすればICカードで利用した事を証明可能とすることができる。

【0017】また、ICカードあるいはICカード端末とセンタが認証等を行うことなく、オフラインでのサービス提供が可能である。

【図面の簡単な説明】

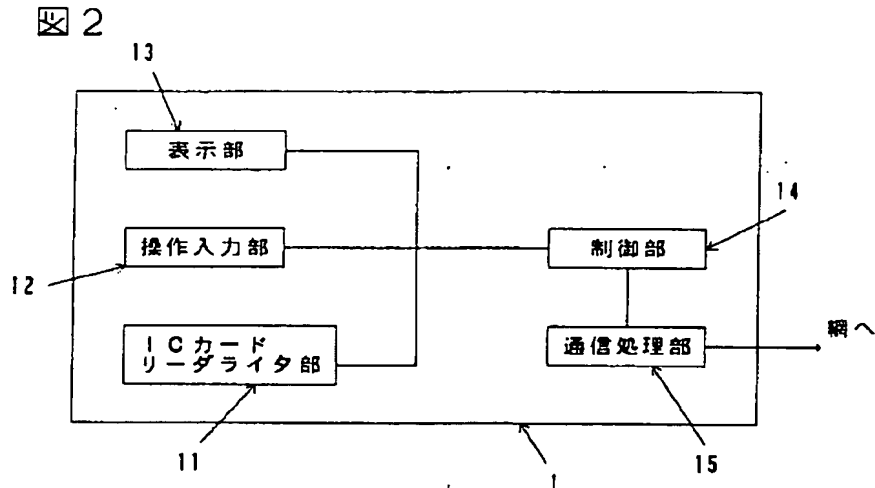
【図1】この発明のシステム構成例を示すブロック図。

【図2】ICカードとICカード端末との間の情報処理、通信手順を示す図。

【図3】ICカード端末の構成例を示すブロック図。

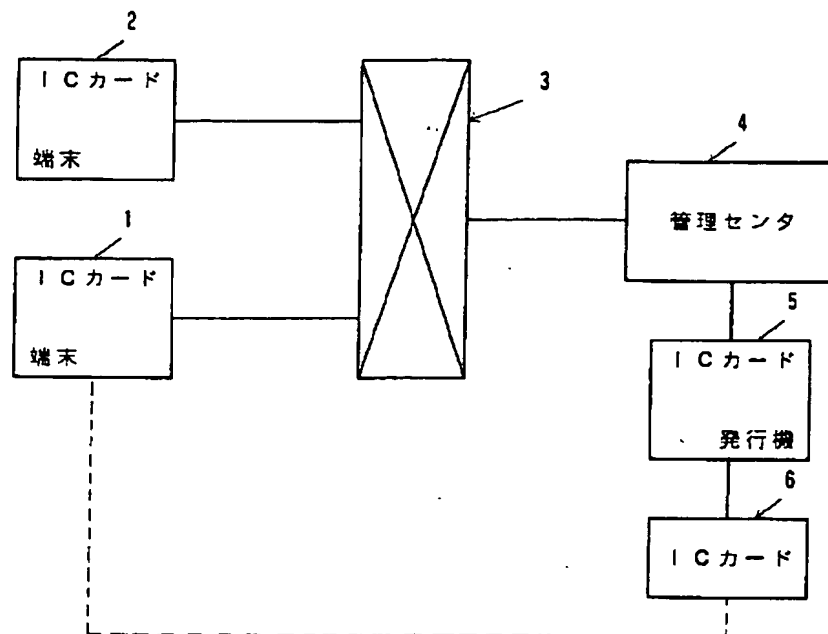
【図4】ICカードの構成例を示す図。

【図2】

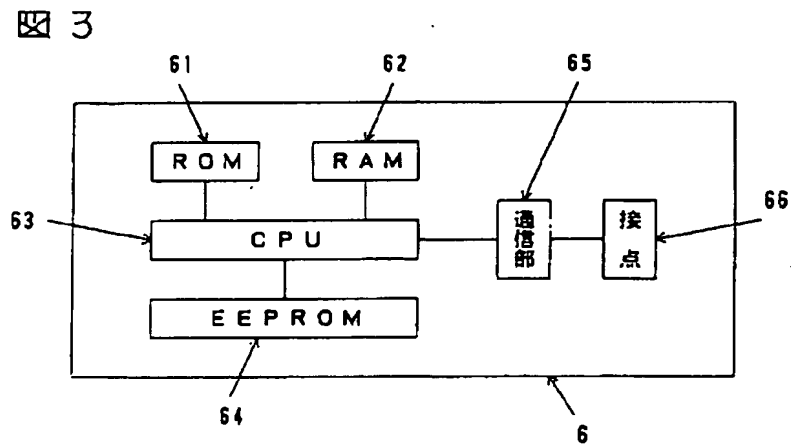


【図1】

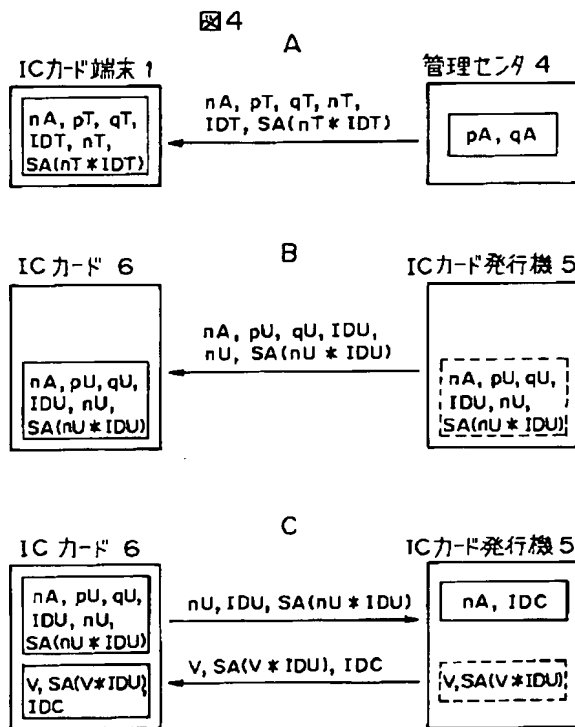
図 1



【図 3】



【図 4】



【手続補正書】

【提出日】平成 4 年 1 0 月 2 8 日

【手続補正 1】

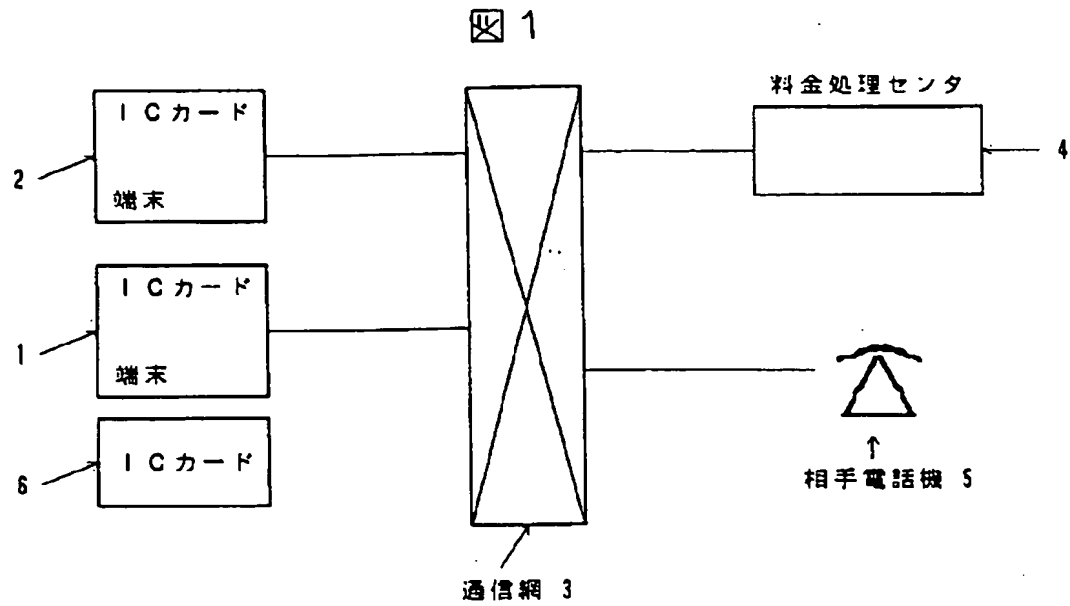
【補正対象書類名】図面

【補正対象項目名】全図

【補正方法】変更

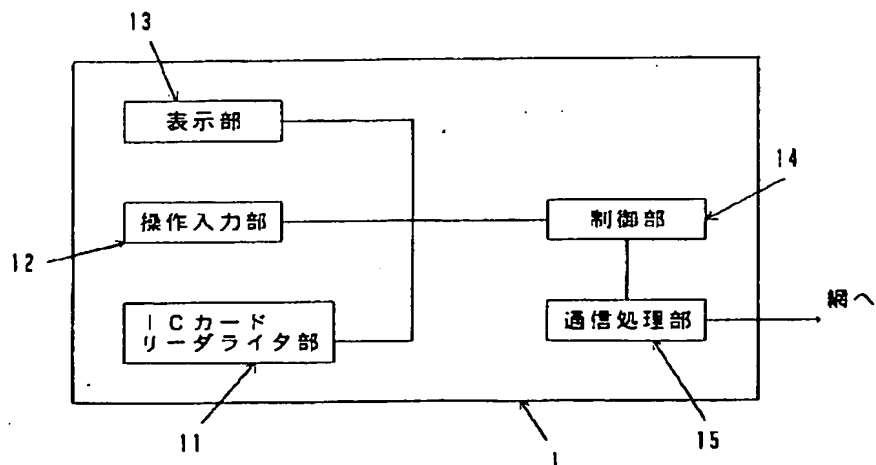
【補正内容】

【図1】



【図3】

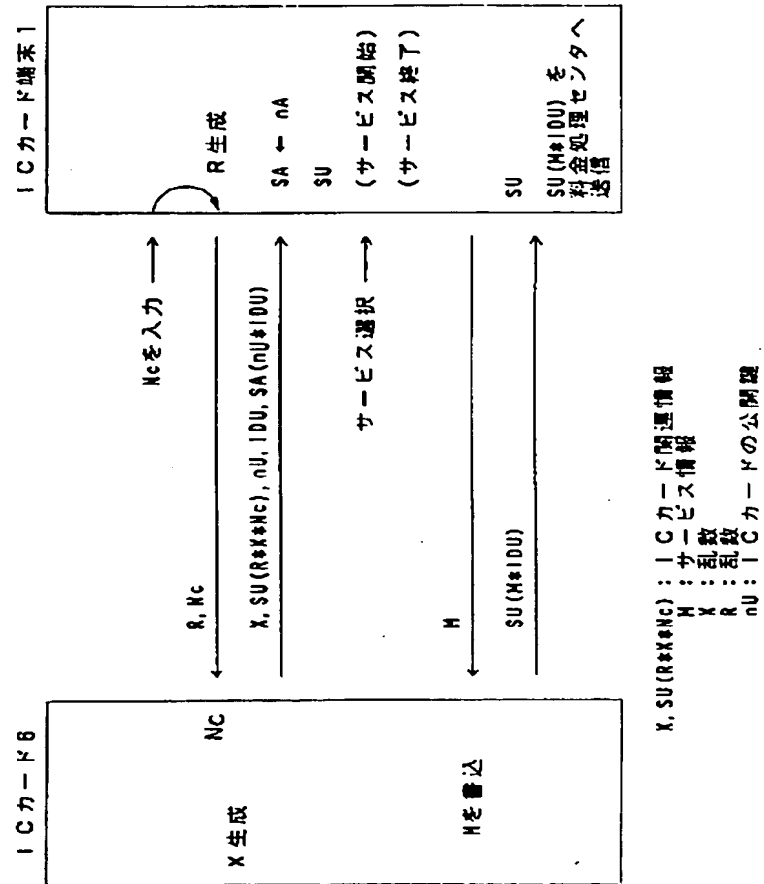
図 3





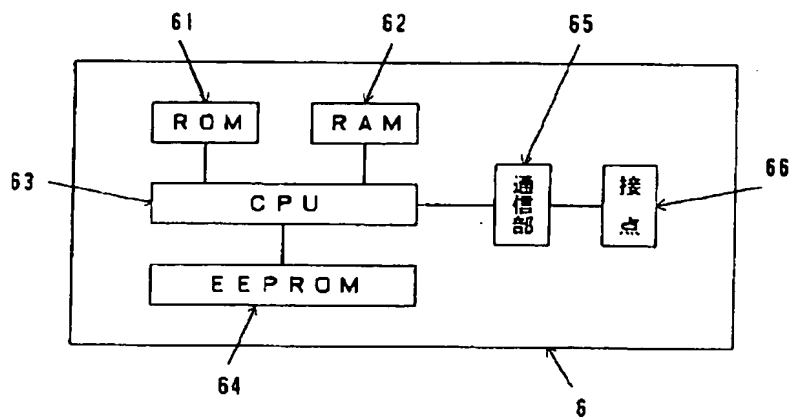
【図2】

図2



【図 4】

4



フロントページの続き

(72)発明者 宮口 庄司  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内

(72)発明者 岡本 龍明  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内

(72)発明者 藤岡 淳  
東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内